

[Ask a Question](#) [Write a Blog Post](#)[Login](#)**Alessandro Banzer**

March 17, 2014 | 1 minute read

Defining Mitigating Controls / Compensating Controls

4 comments 12 likes 37,140 views

[Follow](#)[Like](#)[RSS Feed](#)

Dear all,

in this document I would like to share how mitigating/compensating controls can be defined from a business point of view. The mitigation only leads to desired results when a potential risk is either properly segregated or properly controlled.

Due to an almost unlimited number of potential segregation of duties conflicts it is necessary to define the important conflicts (for your enterprise) and design and build the rules to identify the risks within GRC. Further it is required that the selected SOD conflicts be addressed via segregation of duties or compensating controls.

Furthermore, it is of importance to consider that segregation of duties is only fully achieved when both implementation of segregation within processes (User A creates a record, while User B reviews it) and proper access rights restriction within SAP applications are simultaneously present.

In case segregation of duties cannot be achieved due to a lack of personnel or other reasons, compensating controls (alternative controls) need to be implemented to minimize the risks of accumulation of duties. These detecting controls are less desirable than segregation of duties which is a prevention control. The following lists the various types of compensating controls that management should consider implementing when there is inadequate segregation of incompatible duties:

- **Second signature:** e.g. two signatures required to authorize bank payments, salary transfer initiation, purchase orders, etc.
- **Review by a supervisor:** e.g. the daily journal entries report reviewed and signed by the supervisor of the person responsible for posting the journal entries
- **Exception reports:** these reports should be reviewed in a timely manner, checked against supporting documents evidencing authorization and signed by supervisor. Some examples of reports (preferably SAP standard reports and system-generated):
 - Report of changes performed to G/L accounts -> report of updated/opened GL accounts
 - Report of postings recorded on accruals accounts
 - Report on pending items resulting from reconciliations (e.g. bank reconciliation, G/L and sub-ledgers reconciliations, etc)
 - List of adjustments to a prior period
 - Report of payments above a given threshold
 - Report of changes performed on customer master data
 - etc. etc.
- **Independent detailed review** of transactions for the department or function. For example, when a user can perform all the key activities of a transaction without adequate segregation of duties, an independent review of the detailed transactions for the department has to be performed on a regular basis to identify, investigate and correct improper/erroneous transactions. This must definitely be done by a second, independent person.
- **Random review of transactions:** management should periodically review a sample of transactions and compare against supporting documents

Furthermore, it is highly recommended that compensating controls are reviewed and checked for evidence (e.g. if reports have been reviewed) periodically by an independent person (e.g. internal audit) to ensure that alternative controls are working accordingly.

Looking forward to your input in this regard to get also other views from people who are involved in designing process for compensating controls.

Thanks for reading.

Best regards,

Alessandro



Alert Moderator

Assigned Tags

Retagging required | Governance Risk And Compliance | governance risk and compliance sap grc | grc 10.0 | mitigating control | mitigation | mitigation controls

Similar Blog Posts

[Mitigating controls - is this a cure for \"all evil\" in excessive authorizations risks in SAP? \(part 2/5\)](#)

By Filip Nowak Jan 25, 2023

[Mitigation Controls creation and assignment in SAP GRC 12.0](#)

By Javed Khan Apr 19, 2023

[Mitigating Control Lifecycle](#)

By Alessandro Banzer Feb 23, 2014

Related Questions

[Creating a Mitigating Control For two roles that contain a Risk.](#)

By Former Member Jul 15, 2011

[ARA: Need your suggestion for mitigation of risks???](#)

By Faisal Khan May 19, 2014

[Mitigation controls for self-conflicting transactions](#)

By Former Member Nov 05, 2014

4 Comments

You must be [Logged on](#) to comment or reply to a post.



Former Member

March 18, 2014 at 1:56 pm

Allesandro,

Thanks for sharing your thoughts on mitigating controls.

Perhaps it would be worthwhile to mention that there are three types of business controls

Inherent controls enforced by SAP. Sales orders can not be applied to non-existing customers .

Configurable controls - switches that can be turned on and off in SAP. Eg. purchase invoices are automatically checked against the purchase order and delivery.

Procedural controls - Exception / change log reports

Like 0 | Share



Former Member

October 7, 2015 at 6:40 pm

Hello Allesandro,

Also thanks for sharing. I am currently going over a dispute over mitigating controls.

My understanding is that the mitigating controls are manual controls and not automated controls within SAP.

Have you ever seen an automated control being used as a mitigating control for an SOD?

Thanks,

Like 0 | Share

**Alessandro Banzer** | Blog Post Author

October 8, 2015 at 9:58 am

Dear Carolina,

thanks for your feedback. Automated controls can be implemented with SAP Process Control. Did you check out the functionalities of Process Control so far?

Regards,

Alessandro

Like 0 | Share



Former Member

October 8, 2015 at 2:43 pm

Hello Alessandro,

We have implemented automated controls. The question is if we can use those automated or any SAP automated control as a mitigating control for an System SOD.

Thank you,

Carolina

Like 0 | Share

Find us on



Privacy	Terms of Use
Legal Disclosure	Copyright
Trademark	Cookie Preferences
Newsletter	Support